IN THE CLAIMS:

Please amend claims 1-18 as follows. Please add new claims 19-20 as follows.

1. (Currently Amended) A method ~~of reducing denial of service attacks by malicious mobile nodes in a mobile internet protocol (IP) environment~~, ~~said method~~ comprising:

maintaining, by each of a plurality of access routers within ~~the~~ a mobile ~~IP~~ internet protocol environment, a cache of neighboring access routers as candidates and their associated access points; and

populating ~~the caches~~ each cache with cache entries in response to actions initiated by mobile nodes,

wherein each cache entry is tagged with an identity of an action initiating mobile node, which identity is based on information that is verifiable by the access routers and which cannot be modified arbitrarily by the mobile node, and

wherein a total number of entries that can be tagged and thus introduced into a cache by any given node is limited.

2. (Currently Amended) A method ~~of validating information of a mobile node within a candidate access router discovery procedure in a mobile internet protocol environment~~, ~~said method~~ comprising:

generating a token by a first access router to which ~~the~~ a mobile node was previously attached;

sending the token from the first access router to the mobile node within a message comprising a list of candidate access routers;

sending the token from the mobile node to a second access router as selected candidate after a handover procedure between the first and second access routers; and

sending the token within an exchange between the access routers specific to ~~the~~ a candidate access router discovery procedure from the second access router back to the first access router for verification.

3. (Currently Amended) The method according to claim 1, wherein the identity of the mobile node is an international mobile subscriber identity ~~(IMSI)~~ for cellular communication systems, and a network access identifier ~~(NAI)~~ for systems based on internet protocol ~~(IP)~~.

4. (Currently Amended) The method according to claim 1, wherein an action initiated by a mobile node comprises a handover procedure of the mobile node between a previous access router and a new access router, said method further comprising:

generating a token by the previous first access router;

sending the token from the previous access router to the mobile node within a message comprising a list of candidate access routers;

sending the token within a message specific to ~~the~~ a candidate access router discovery procedure from the mobile node to the new access router as a selected candidate after the handover procedure;

sending the token within a neighbor exchange between the access routers resulting in cache entries being created or refreshed from the second access router back to the first access router for verification.

5. (Currently Amended) The method according to claim 4,

wherein the token is generated by maintaining by the previous access router a short list of random values used as keys to hash the identity of the mobile node,

wherein each key in the short list is associated with an integer index that is passed along with the token, and

wherein upon receiving the token for verification, the previous access router uses the integer index to lookup the associated key, hash the identity of the mobile node sent in the neighbor exchange and compares the hash to the token.

6. (Currently Amended) The method according to claim 5, wherein with progressing time new keys are generated and added to the head of the list while old keys are expired and removed so that from the length of the list and the frequency of generated keys, the total amount of time ~~is determined~~ a mobile has been attached is determined.

7. (Currently Amended) A system ~~for reducing denial-of-service attacks by malicious mobile nodes in a mobile internet protocol (IP) environment~~, ~~said system~~ comprising:

a plurality of access routers within ~~the~~ a mobile ~~IP~~ internet protocol environment, each router configured to maintain a cache of neighboring access routers as candidates and their associated access points; and

a plurality of mobile nodes which are capable of populating the caches in response to actions initiated,

wherein the cache is configured such that each cache entry is tagged with an identity of the action initiating mobile node having thus created the entry, and that a total number of entries that can be tagged and thus introduced into the cache by any given node is limited.

8. (Currently Amended) A system ~~for validating information of a mobile node within a candidate access router discovery procedure in a mobile internet protocol environment~~, ~~the system~~ comprising:

a first access router;

~~said~~ a mobile node; and

a second access router,

wherein, the first access router ~~includes~~ comprises a generating unit configured to generate a token, and a first sending unit configured to send the token to the mobile node within a message comprising a list of candidate access routers, ~~and~~

wherein the mobile node ~~includes~~ comprises a second sending unit configured to send the token to the second access router as selected candidate after a handover procedure between the access routers, and

wherein the second access router ~~includes~~ comprises a third sending unit configured to send the token within an exchange between the access routers specific to ~~the~~ a candidate access router discovery procedure back to the first access router and a verification unit configured to verify the token.

9. (Currently Amended) The system according to claim 7,

wherein ~~the access routers~~ each access router ~~include~~ comprises a ~~generating unit~~ generator configured to generate a token, a first ~~sending unit~~ sender configured to send the token to a mobile node within a message comprising a list of candidate access routers, a second ~~sending unit~~ sender configured to send the token within a neighbor exchange between access routers resulting in cache entries being created or refreshed, and a ~~verification unit~~ verifier configured to verify the token[[;]], and

wherein the mobile ~~nodes include~~ node comprises a third sending unit configured to send the token to a new access router as a selected candidate after a handover procedure.

10. (Currently Amended) The system according to claim 9,

wherein the ~~generating unit~~ generator ~~includes~~ comprises a first hashing unit configured to hash the identity of the mobile node by using random values out of a short list as keys, and an associating unit configured to associate each key in the list with an integer index, and

wherein the ~~verification unit includes~~ verifier comprises a lookup table for the indices and their associated keys, a second hashing unit configured to hash the identity of the mobile node and a comparing unit configured to compare the hash to the token.

11. (Currently Amended) The system according to claim 10,

wherein the ~~generating unit~~ generator is configured to generate new keys with progressing time, to add them to the head of the list, and to remove old keys[[;]].

the system further comprising

a ~~determination unit~~ determiner configured to determine a total amount of time a mobile has been attached from the length of the list and the frequency of generated keys.

12. (Currently Amended) ~~An access router~~ An apparatus~~for reducing denial-of-service attacks by malicious mobile nodes in a mobileinternet protocol~~, ~~said router~~ comprising:

a cache of neighboring access routers as candidates and their associated access points,

wherein the cache is ~~arranged~~ configured such that each cache entry is tagged with ~~the~~ an identity of ~~the~~ a mobile node having initiated the entry creation, and that the total number of entries that can be tagged and thus introduced into the cache by any given node is limited.

13. (Currently Amended) ~~An access router~~ An apparatus~~for validating information of a mobile node in a mobile~~internet ~~protocol~~, comprising:

a ~~generating unit~~ generator configured to generate a token;

a first ~~sending unit~~ transmitter configured to send the token to the mobile node within a message comprising a list of candidate access routers;

a second ~~sending unit~~ transmitter configured to send the token within an exchange with another access router specific to ~~the~~ a candidate access router discovery procedure to the other access router; and

a ~~verification unit~~ verifier configured to verify the token.

14. (Currently Amended) The ~~access router~~ apparatus according to claim 12, further comprising:

a ~~generating unit~~ generator configured to generate a token,

a first ~~sending unit~~ transmitter configured to send the token to a mobile node within a message comprising a list of candidate access routers,

a second ~~sending unit~~ transmitter configured to send the token within a neighbor exchange with another access router resulting in cache entries being created or refreshed, and

a ~~verification unit~~ verifier configured to verify the token.

15. (Currently Amended) The ~~access router~~ apparatus according to claim 14,

wherein the ~~generating unit includes~~ generator comprises a first hashing unit configured to hash the identity of the mobile node by using random values out of a short list as keys, and an associating unit configured to associate each key in the list with an integer index, and

wherein the ~~verification unit includes~~ verifier comprises a lookup table for the indices and their associated keys, a second hashing unit configured to hash the identity of the mobile node and a comparing unit configured to compare the hash to the token.

16. (Currently Amended) The ~~access router~~ apparatus according to claim 15, wherein the ~~generating unit~~ generator is configured to generate new keys with progressing time, to add them to the head of the list, and to remove old keys.

17. (Currently Amended) A system ~~for validating information of a mobile node within a candidate access router discovery procedure in a mobile internet protocol environment~~, comprising:

a first access router[[,]];

~~said~~ a mobile node; and

a second access router,

wherein[[:]] the first access router ~~includes~~ comprises generating means for generating a token, and first sending means for sending the token to the mobile node within a message comprising a list of candidate access routers,

wherein the mobile node ~~includes~~ comprises second sending means for sending the token to the second access router as selected candidate after a handover procedure between the access routers, and

wherein the second access router ~~includes~~ comprises third sending means for sending the token within an exchange between the access routers specific to ~~the~~ a candidate access router discovery procedure back to the first access router and verification means for verifying the token.

18. (Currently Amended) An apparatus ~~for validating information of a mobile node in a mobileinternet protocol~~, comprising:

generating means for generating a token;

first sending means for sending the token to ~~the~~ a mobile node within a message comprising a list of candidate access routers;

second sending means for sending the token within an exchange with another access router specific to ~~the~~ a candidate access router discovery procedure to the other access router; and

verification means for verifying the token.

19. (New) A method, comprising:

generating a token by a first access router to which a mobile node was previously attached; and

sending the token from the first access router to the mobile node within a message comprising a list of candidate access routers,

wherein the token is sent from the mobile node to a second access router as selected candidate after a handover procedure between the first and second access routers, and

wherein the token is sent within an exchange between the access routers specific to a candidate access router discovery procedure from the second access router back to the first access router for verification.

20. (New) The method according to claim 1, wherein an action initiated by a mobile node comprises a handover procedure of the mobile node between a previous access router and a new access router, said method further comprising:

generating a token by the previous first access router; and

sending the token from the previous access router to the mobile node within a message comprising a list of candidate access routers,

wherein the token is sent within a message specific to a candidate access router discovery procedure from the mobile node to the new access router as a selected candidate after the handover procedure, and

wherein a token is sent within a neighbor exchange between the access routers resulting in cache entries being created or refreshed from the second access router back to the first access router for verification.